International Journal of Electronics Communication and Computer Engineering
Volume 6, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Survey on Security and Privacy Issues in Mobile Cloud Computing Environment

Dr. M. Gopichand
Professor & Head, Department of IT, Vardhaman College of Engineering, Shamshabad A.P, INDIA.
email:gopi_merugu@yahoo.com

***Abstract*—Mobile cloud computing is a computing which involves interaction of mobile devices with cloud computing environment. This paper overviews the major concerns of security problems and privacy issues of mobile users with cloud environment. It highlights the data security issues and discusses the privacy model of mobile cloud computing environment. It brings several advantages to the devices with low resources; advantages that lead to the development of rich functionality applications. The security issues in Mobile Cloud Computing can be classified as follows: mobile threats and cloud threats. The main purpose of these menaces is to steal personal data (e.g. credit card numbers, passwords, contact database, calendar, location) or to exploit mobile device resources.**

***Key Words*— Cloud Computing Security, Mobile Cloud Computing Security, Data Security, Privacy Protection.**

I. INTRODUCTION

The Mobile cloud computing is the usage of cloud computing in combination with smart mobile devices. Cloud computing exists when tasks and data are kept on the internet rather than on individual devices, providing on-demand access of data. Its key characteristics include agility, reduced Cost, device independence, reliability (multiple redundant sites), scalability, security and reduced maintenance. It is already a permanent fixture of consumer oriented services such as email, storage and social media [4]. The opportunities provided by cloud computing becomes available to enterprises of all sizes that enables them to deliver more scalable and resilient services to employees, partners and customers at lower cost and with higher business agility [1].

Mobile cloud computing refers to the availability of cloud computing services in a mobile environment. It incorporate the elements of mobile networks and cloud computing, thereby providing optimal services for mobile users. In mobile cloud computing, mobile devices do not need a powerful configuration (e.g., Cusped and memory capacity) since all the data and complicated computing modules can be processed in the clouds [2, 5].

The more and more information that is placed in the cloud by individuals and enterprises, the more and more they become vulnerable to attacks and data is lost and privacy is not preserved for mobile users.

II. DEFINITIONS

Mobile Cloud Computing (Fig.1) is a new concept that can be described as the availability of Cloud Computing resources and services for mobile devices. As in the case of Cloud Computing, several definitions were proposed to define Mobile Cloud Computing.

Mobile Cloud Computing is defined in [4] as follows:

"Mobile cloud computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smart-phone users but a much broader range of mobile subscribers."

Another definition given in [5]:

"Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions, while preserving available

III. CLOUD COMPUTING SECURITY

Traditional security issues are still present in cloud computing environments. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in cloud. Due to the openness and multi-tenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field:

(1) Due to dynamic scalability, service abstraction, and location transparency features of cloud computing models, all kinds of applications and data on the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it's difficult to isolate a particular physical resource that has a threat or has been compromised.

(2) According to the service delivery models of cloud computing, resources cloud services based on may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measures.

(3) As the openness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by other unauthorized users.

(4) As the cloud platform has to deal with massive information storage and to deliver a fast access, cloud security measures have to meet the need of massive information processing.

According to the SPI service delivery models, deployment models and essential characteristics of cloud, there are security issues in all aspects of the infrastructure including network level, host level and application level.

International Journal of Electronics Communication and Computer Engineering
Volume 6, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

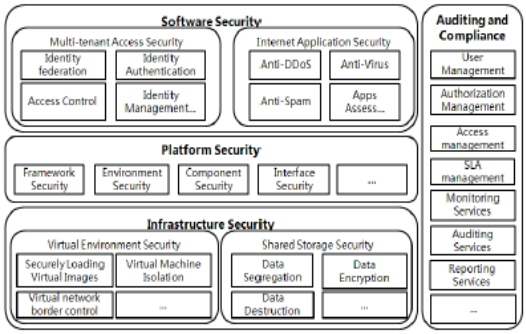

Fig-1:Cloud Computing Security Architecture Sensing And Interactivity Capabilities Of Mobile Devices

IV. Cloud Computing Service Delivery Models and Security Implications

A. IaaS Issues

VM security – securing the VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud-oriented security solutions. The VM's security is the responsibility of cloud consumers. Each cloud consumer can use their own security controls based on their needs, expected risk level, and their own security management process.

Securing VM images repository - unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that such templates may retain the original owner information which may be used by a new consumer.

Virtual network security - sharing of network infrastructure among different tenants within the same server (using vSwitch) or in the physical networks will increase the possibility to exploit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities, or even the vSwitch software which result in network-based VM attacks.

Securing VM boundaries - VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing VM boundaries is the responsibility of the cloud provider.

Hypervisor security - a hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice versa. It is the main controller of any access to the physical server resources by VMs. Any compromise of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted. Hypervisor security is the responsibility of cloud providers and the service provider. In this case, the SP is the company that delivers the hypervisor software such as VMware or Xen.

B. PaaS Security Issues

SOA related security issues – the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks [9, 16]. Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services. This security issue is a shared responsibility among cloud providers, service providers and consumers.

API Security - PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented, such as OAuth [17], to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

C. SaaS Security Issues

In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them including data security management [11] (data locality, integrity, segregation, access, confidentiality, backups) and network security.

Web application vulnerability scanning - web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners [18]. Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE) [19]. Web application firewalls should be in place to mitigate existing/discovered vulnerabilities (examining HTTP requests and responses for applications specific vulnerabilities). The ten most critical web applications vulnerabilities in 2010 listed by OWASP [20] are injection, cross site scripting (Input validation) weaknesses.

Web application security miss-configuration and breaking - web application security miss-configuration or weaknesses in application-specific security controls is an important issue in SaaS. Security miss-configuration is also very critical with multi-tenancy where each tenant has their own security configurations that may conflict with each other leading to security holes. It is mostly recommended to depend on cloud provider security controls to enforce and manage security in a consistent, dynamic and robust way.

D. Cloud Management Security Issues

The Cloud Management Layer (CML) is the "microkernel" that can be extended to incorporate and coordinate different components. The CML components include SLA management, service monitoring, billing,

International Journal of Electronics Communication and Computer Engineering
Volume 6, Issue 3, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

elasticity, IaaS, PaaS, SaaS services registry, and security management of the cloud. Such a layer is very critical since any vulnerability or any breach of this layer will result in an adversary having control, like an administrator, over the whole cloud platform.

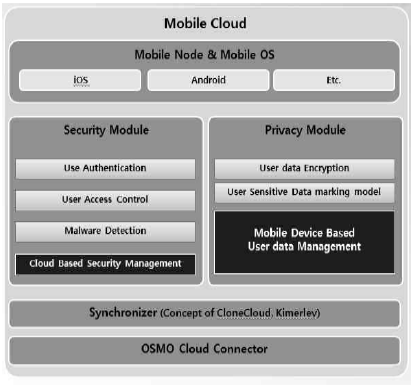

Fig-2:Mobile Cloud Computing Security Architecture. Architecture.

IV. Mobile Cloud Computing Security

The one of the key issues that most cloud providers are given attention is securing mobile cloud computing is user's privacy and integrity of data or applications. Subsequently mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are classified into two categories:

- Mobile network user's security
- Cloud security

Mobile network security: Different mobile devices have numbers of security threats such as malicious codes some applications to these can cause privacy issues for mobile users .There are two main issues concerning the mobile user security

Mobile Application Security: - The easiest ways to check security problems is done by installing and running security software and antivirus on mobile devices. But since mobile devices are having limitation with processing and power, protecting them from these threats could be more difficult compared to regular computers. Several techniques have been introduced for transferring threat detection and security mechanisms to the cloud. Before mobile users could use an application, it should go through some level of threat evaluation. All file activities that are done on mobile devices will be verified if it is malicious or not. Instead of running antivirus software or threat detection programs locally, mobile devices only performs lightweight activities such as execution traces transmitted to cloud security servers.[8]

Privacy: Revealing your private information such as giving geo location and user's important Information like date of birth, Credit card information etc. creates situations for privacy issues. For example, use of GPS on mobile devices. Intimidations for revealing private information could be reduced through selecting and analyzing the enterprise needs and require only specified services to be acquired and moved to the cloud [8].

VI. Data Security and Privacy Model For Mobile Cloud Computing

Mobile devices are famous for malicious code. There are many chances to lose or steal the data because mobile devices are mostly unprotected. An unauthorized person can easily access the information stored on the mobile devices. The top mobile threats that affect security are

1. Data loss from lost/ stolen devices.
2. Information stealing by mobile malware.
3. Data leakage through poorly written third party applications.
4. Vulnerabilities within devices, OS, design and third-party applications.
5. Insecure network access and unreliable access points.
6. Insecure or rogue marketplaces.
7. Insufficient management tools, capabilities and access to APIs.
8. Near Field Communication (NFC) and proximity-based hacking.

Data can be sniffed by the intruders during wireless communications. Data access can be interrupted due to multiple points. This leads to the data locked in particular services. To protect the mobile devices from data loss, thin client like anti-malware, antivirus should be installed to monitor the malicious code. Malicious code includes not only viruses but also phishing from malicious social networks and domains, botnets, spam and identity theft. Wireless protocol encryption provides secured communication where intruders cannot hack the network.

Security and privacy are always a key issue when the data are shared between mobile devices and the cloud. Even though WPA2 (Wi-Fi Alliance, 2012) provides layer-2 encryption of the data, layer-6 encryption is still a requirement because it requires some external applications like bioinformatics or computational chemistry that are executed on mobile devices and remotely on rented/ commercial cloud platforms (such as Google (2012, AWS (2012), Microsoft (2012)) which require an additional layer

A. Data Security Issues In The Mobile Cloud

Privacy and Confidentiality:

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

Data Integrity:

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain

dataset and at what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

Data Location and Relocation:

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information.

Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each other's' resources.

Data Availability:

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

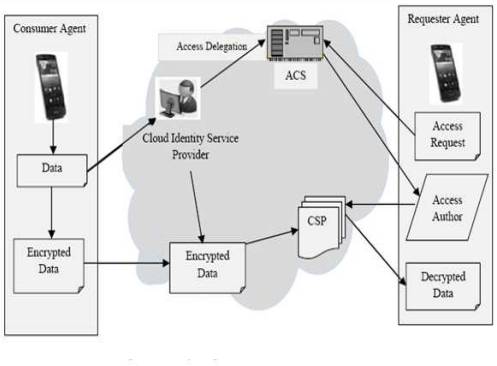

Fig-3: Privacy Design Model for Mobile Cloud

B. Privacy Design By Mobile Cloud

The Fig-3 shows a likely minimalist of mobile cloud computing architecture that maintains privacy and usability when data is encrypted and outsourced into the Cloud.

This proposed architecture is mainly designed to overcome one of the challenging problems, this model ensuring that organizations that make legitimate requests are granted access to encrypted data. This architecture needs to collaborate between two agents the consumer's agent and the requestor's agent and two service providers the Cloud access control service provider (ACSP) [14] and the Cloud data service provider (DSP).

The consumer's agent encrypts data prior to sending it to the Cloud DSP, and issues access delegation to the Cloud ACSP that will handle data utilization requests from the requestor. When one party wants to access the data through his or her mobile device, he or she contact the cloud access control service provider for access authorization, for the sake of privacy protection requester would not go directly to the Cloud DSP [15]. Upon authentication of the requestor, and satisfaction of any criteria set out in the access delegation, the Cloud ACSP would issue an access authorization to the requestor.

This proposed authorization message would consist of three components, each with a different effect. First, it would indicate to the Cloud DSP that the requestor had been authenticated, and was permitted to access the consumer's data. Second, the Cloud ACSP would include in the message any available information regarding the subset of data to be released to the requestor, with the goal of restricting requestor access to be only the minimum required for its stated purposes.

Finally, the authorization message would also contain a decryption key for the released data, engineered so as to only allow the requestor decrypt capabilities. Should the requestor be able to circumvent this system, contacting the Cloud DSP directly and managing to succeed in retrieving data, the absence of the appropriate decryption key implies that all that is retrieved is meaningless cipher text. Similarly, if the Cloud DSP were compromised or actively.

VII. CONCLUSION

According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible

The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the mobile internet has become a growing concern. These concerns include whether personal information can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited.

The key to privacy protection in the mobile cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements. According to the analysis for data security and privacy protection issues above, it is expected to have an integrated and comprehensive security solution to meet the needs of defense in depth. Regarding privacy protection, privacy data identification and isolation are the primary tasks. They should be considered during the design of mobile cloud-based applications.

VIII. FUTURE WORK

For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order tonsure no un-authorized access to organizations' cloud resources by some employees who has left the organizations. Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed

REFERENCES

[1] D. Kovachev, Yiwei Cao and Ralf Klamma. Mobile Cloud Computing: "A Comparison of application Models". In eprintar Xiv: 1107.4940, July 2011.
[2] S.K.Sood, "A combined approach to ensure data security in cloud computing", in S.K. Sood/Journal of Network and Computer Applications Vol.35, pp. 1831–1838, 2012.
[3] S. Chetan, G. Kumar, K. Dinesh, K. Mathew and M. A. Abhimanyu "Cloud Computing for Mobile World", available online: http://chetan.ueuo.com/projects/CCMW.pdf. 2010.
[4] Mobile Cloud Computing Forum, available online: http://www.mobilecloudcomputingforum.com
[5] White Paper, "Mobile Cloud Computing Solution Brief," AEPONA, November 2010.
[6] R. D. Caytiles, S. Lee, "Security Considerations for Public Mobile Cloud Computing", International Journal of Advanced Science and Technology Vol. 44, July, 2012.
[7] S.K. Ko, J.H. Lee, S.W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering,2012.
[8] S. Subashini, V.Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(2011)1-11.
[9] Mohamed Al Morsy, John Grundy, Ingo Müller, "An Analysis of The Cloud Computing Security Problem," in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.
[10] Yanpei Chen, Vern Paxson, Randy H. Katz, "What's New About Cloud Computing Security?"Technical Report No. UCB/EECS-2010-5.
[11] Roy I, Ramadan HE, Setty STV, Kilzer A, Shmatikov V, Witchel E."Airavat: Security and privacy for Map Reduce," In: Castro M, eds. Proc. of the 7th Usenix Symp. on Networked Systems Design and Implementation. San Jose: USENIX Association, 2010. 297.312.
[12] Zeng K, "Publicly verifiable remote data integrity," In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 2008.419.434.
[13] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 17thInternational Workshop on Quality of Service.2009:1-9.
[14] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16thACM Computer and Communications Security Conf., CCS 2009. NewYork: Association for Computing Machinery, 2009. 43.54. [doi:10.1145/1655008.1655015]
[15] Muntés-Mulero V, Nin J. Privacy and anonymization for very large datasets. In: Chen P, ed. Proc of the ACM 18th Int'l Conf. on Information and Knowledge Management, CIKM 2009. New York: Association for Computing Machinery, 2009.2117.2118. [doi:10.1145/1645953.1646333]